REMARKS/ARGUMENTS

Favorable reconsideration and allowance of claims 12, and 13-17, as amended, is respectfully requested.

The Examiner's provisional rejection of claims 1-20 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 16 of co-pending Application No. 09/505,830 is respectfully traversed. Applicant is submitting herewith a Terminal Disclaimer and the required fee of $130.00 to obviate the Examiner's provisional double patenting rejection over claim 16 of co-pending Application No. 09/505,830. The Terminal Disclaimer is signed by the Attorney of Record in the subject patent application, the undersigned attorney.

The specification is being amended to add the reference characters, noted by the Examiner in the above office action, in the written description in compliance with 37 CFR 1.121(b). Specifically, the paragraph beginning at page 7, line 15 is being amended to describe the waveforms of FIGS. 3A, 3B and 3C. The specification, as amended, beginning at page 13, line 1, also describes the erase key() routine 56 (illustrated in FIGS. 4 and 8). The program steps of reference numerals 76 and 80 (FIG. 6) are described in the paragraph beginning at page 9, line 13. The

program step of reference numeral 122 (FIG. 8) is described in the paragraph beginning at page 13, line 16.

A new paragraph is being added to the specification beginning at page 14, line 2 to describe each of the program steps of FIG. 9 which depicts the interrupt handler() routine 130. No changes are being made to the drawings by this amendment.

The specification is also being amended at page 5, line 23 and page 8, lines 1 and 3 to correctly describe encryption unit 24 as a KGV-68 encryption unit.

The Examiner's objections to claims 1 and 12 are being corrected by this amendment. Claim 1 and the claims dependent therefrom are being canceled by this amendment. The spelling of the word "microcontroller" has been corrected at lines 18 and 24 of claim 12. In claim 13, line 5, the phrase "check word" is now --said check word--. In claims 15 and 17, line 2, the word "said" has been deleted. Claim 20 is being canceled by this amendment.

Claims 1-11 are being canceled by this amendment. Therefore any rejection of these claims under 35 U.S.C. 103(a) is no longer applicable to these claims.

The Examiner's rejection of claim 12 under 35 U.S.C. 103(a)

as being unpatentable over Rollingson et al. (U.S. 5,156,357) in view of Borgen (H1414) in view of Best (U.S. 4,278,837) in view of Maher (U.S. 5,513,261) in view of Le et al. (U.S. 5,883,956) further in view of Tu et al. (U.S. 5,682,403) is respectfully traversed. The Examiner asserts that Rollingson et. al. discloses a missile telemetry system without an encryption system and that the encryption system of Best could be used in the telemetry system of Rollingson.

To establish obviousness by combining the teachings of the prior art to produce the claimed invention, there must be some teaching, suggestion or incentive supporting the combination. The prior art Rollingson patent makes no mention of an encryption device. Best specifically discusses its encryption device as being useful for computer program protection in compact, lightweight microcomputers. The intent of the Best device is to prevent unauthorized use of proprietary information contained in computer programs which are executed by a computer. Theft of such information by an individual or individuals may result in the program being widely distributed by the pirate(s) such that the program can no longer be a trade secret. See for example. the Description of the Prior Art, column 1, lines 40-64. Further, the Objects of the Invention make it very clear, that

the object of the invention of Best is "to protect a program from discovery by a person who has access to the writing of the computer in which a copy of the program is executed".

Accordingly, it is respectfully submitted that there is no teaching, motivation or suggestion in Best for the proposed combination since Best teaching is limited to the encryption of microprocessor executed computer programs stored in cipher. There is simply no teaching, motivation or suggestion in Best for the Examiner's proposed combination since Best makes no mention of using his invention other than for protecting a microprocessor's internal software from piracy. Without the benefit of Applicants' teachings, i.e. use of an encryption with key load and erase capabilities in a missile's telemetry system for encrypting telemetry data, it is submitted that the Examiner could not make his proposed combination.

Further, the Examiner's proposed combination would suggest to one of ordinary skill in the art that the computer software illustrated in FIGS 4-9 and now recited in amended claim 12 should be encrypted to protect the software from piracy. This is not the purpose of Applicants' invention. Applicants only purpose is protect the missile's telemetry data from compromise.

The Examiner asserts that Best teaches the method step of

limitation (j) of claim 12 which recites erasing the crypto key from the memory upon the launch of the missile. The teaching of Best beginning at column 5, line 62 and continuing through column 6 line 11 is directed to a program which includes disabling instructions in the microprocessor's instructions which erase not only the cipher key but other essential information when an attempt is made to alter the microprocessor's instructions. The teaching of Best is not the recited function in method step (j), i.e. erasure of the crypto key and associated checkword only when there is a missile launch. The teaching of Best would suggest to one of ordinary skill in the art that the erasure would occur only when there is attempt to alter the software program used in microprocessor 32 and not necessarily when there is a missile launch. This is an extremely important claim limitation which the prior art does not teach or even suggest.

The Examiner also asserts that the prior art Best patent teaches method steps (e) and (h) of claim 11 which recite storing the key in the memory of a microcontroller and then loading the key in the memory of the microcontroller into the encryption device for the purpose of encrypting telemetry data transmitted by the missile's telemetry system to a ground station.

Column 14 of Best specifically states that the key is stored

in the CMP (microprocessor) chip 16 and also is made available to an address scrambler 186 which is internal to enciphering unit 184. The unit 184 disclosed in Best is one unitary structure which not only generates the key using random number generator 188 but loads the key into its own address scrambler 186. A key loader 162 within unit 184 loads the key into a circuit board 183 upon which are mounted a memory 12 and CMP 16. A master copy of the computer software program to be encrypted is stored in a separate memory 160. Data bytes of the unenciphered program stored in memory 160 are enciphered as they are written into memory 12 to protect the program from theft or piracy.

The address scrambler 186 produces a scrambled address on a bus 187 which is Exclusive-ORed with a program byte (from memory 160) on bus 180 by gates 182 to produce a cipher byte on bus 165. The cipher byte is then stored in memory 12 at an address specified on an address bus 164. This cycle continues until all program bytes stored in memory 160 are enciphered and stored in memory 12.

Applicants' invention, as recited in amended claim 12, provides for the generation of key by a key loader 22 (method step (a)) which is then stored in the memory of a microcontroller 32 until needed by an encryption device 24 (method step (e)).

Method step (h) provides for a loading the crypto key from the memory of microcontroller 32 into encryption device 24 which encryptes telemetry data transmitted to a ground station by the telemetry system of the missile.

Applicants' respectfully submit step (e) is missing from Best since there is no storage of the key in a memory until it is needed by the gates 182 which perform the encryption function on the unencrypted program stored in memory 160 of Best. The memory storage function is critical to the operation of Applicants' claimed invention since years may lapse before the missile is launched and there is a need for the key by encryption device 24.

Further, the specific functional language of step (h) wherein the key is used by the encryption device 24 to encrypt the missile's telemetry data is not taught by Best. Best teaches generally the encryption of computer programs to prevent access by pirates or individuals not authorized to access the program.

The Examiner asserts that the Tu et al. patent teaches the control of a transmitter during the transfer of the key from the key loader to the memory of the microcontroller, as recited in method steps (c) and (f), and then from the memory the microcontroller to the encryption unit as recited in method steps (g) and (i).

The Tu et al patent discloses a communications network including a base station which turns off its transmitter 40 only at start-up. This allows the processor 80 to perform its self test and other required procedures before the base station 10 can become operational in the network. The transmitter 40 is then turned on and the transmitter proceeds to transmit a TDMA frame of data.

Applicants' claimed invention recites that each transfer of the crypto key requires the transmitter to first being turned off prior to the transfer and then be turned on at the completion of the transfer. The purpose of turning off the transmitter is not to allow the microcontroller of Applicants' claimed invention to perform a self test to insure it is fully operational as taught by the Tu et al patent, but rather to prevent the compromise of classified telemetry information by an accidental transmission of the crypto key used in the missile.

Further, Tu et al. requires that the transmitter being turned off only once during start-up, while Applicants' invention requires that the transmitter being turned off and then on twice, i.e. the first time during the transfer of the crypto key from the key loader to the microcontroller and the second time during the transfer of the crypto key from the microcontroller to the

encryption unit.

Tu et al., in effect, teaches away from the invention of claim 12 in that the Tu et al. patent suggest to one of ordinary skill in the art that the transmitter can remain on after the processor completes its self test and other required procedures before the base station becomes operational. If the transmitter of Applicants' claimed invention were turned off only during system initialization (program steps 40 and 42 of FIG. 4), the result would be a disaster in that classified information would be compromised during the operational portion of the claimed invention which includes the transfer of the crypto key from the key loader 22 to the memory of microcontroller 32 (program steps 44, 46 and 48 of FIG. 4), and the subsequent transfer and loading of the key from the memory of microcontroller 32 to the encryption device 24 (program steps 50, 52 and 54 of FIG. 4).

Claim 12, as amended, now recites the method step (k) of providing a computer software program (illustrated in FIGS. 4-9) executable by microcontroller 32 to perform the functions of method steps (a)-(j). These steps included generating the crypto key (step (a)); the transfer of the crypto key from the key loader 22 to the memory of microcontroller 32 (step (b)); the subsequent transfer and loading of the key from the memory of

microcontroller 32 to the encryption device 24 (step (h)); and the disabling and enabling of the transmitter during the key loading process (steps (c), (f), (g) and (i)). The computer software when executed by microcontroller 32 also performs the steps of duplicating the crypto key (step (d)), storing the crypto key (step (9)) and erasing the crypto key (step (j)).

In the past the loading of a crypto key into a missile's telemetry system encryption unit was accomplished by a hard wired digital logic circuit like the circuitry disclosed in Borgen. Borgen teaches a sequencing control circuit 75 connected to an external EPROM 332 and a static RAM 78. The sequencing control circuit 75 is connected to the power control circuit 41 and the RAM interface circuit 76 of Fig. 1A. The external EPROM 332 is also connected to the power control circuit 41 and the RAM interface circuit 76 of Fig. 1A.

Static RAM 78 receives and stores a key word from a loader 276. Sequencing control circuit 75 provides logic signals for controlling read and write operations of static RAM 78, as well as logic signals to allow for transfer or down loading of the key word from the loader 276 to the static RAM 78.

Borgen also teaches sequencing control circuit 75 as providing logic signals to interface with an encryption device

286 which allows the key word to be transferred or up loaded from the static RAM 78 to the encryption device 288.

The EEPROM 332 of Borgen provides program instructions which control the sequence of operation within the nonvolatile memory system including static RAM 78. Addressing for the EEPROM 332 is provided by sequencing control circuit 75.

The digital hardware/digital logic circuitry for sequencing control circuit 75 is depicted in detail in FIG. 10. The digital logic circuitry of FIG. 10 includes ten bit parallel loadable up counter 140, four eight bit latches 180, 206, 208, and 210, control circuit 168, eight by two bit comparator 250, eight-to-one multiplexer circuit 262, Johnson counter 110, eight bit binary counter 230, eleven bit binary counter 182, and four-to-one demultiplexer 334.

Further, the control circuit 168 for sequencing control circuit 75 includes the 26 logic gates illustrated in Figs. 23A-23F.

The entire non-volatile memory system disclosed in Borgen includes the numerous logic elements illustrated in Figs. 1A (29 logic elements), Fig. 11 (12 logic elements comprising Johnson counter 110), Fig. 13 (20 logic elements comprising counter 140), Fig. 16 (11 logic elements comprising counter 182),

Fig. 14 (5 logic elements comprising each of the ten load circuits 162 in Fig. 13), Fig. 17 (8 logic elements comprising each of the latches 180, 206, 208 and 210 of Fig. 10), Fig. 18 (8 logic elements comprising multiplexer circuit 262 of Fig. 10), Fig. 19 (the eight one bit comparator circuits 252 which make up comparator 250 of Fig. 10), Fig. 21 (the logic elements which make up multiplexer circuit 262), Fig. 23A-23F (26 logic elements which make up control circuit 168 of Fig. 10), and Fig. 31 (the logic elements which make up demultiplexer 334 of Fig. 10).

Except for the EEPROM 332 and the static RAM 78, the nonvolatile memory system of Borgen is made of NAND gates, NOR gates, inverters, flip-flops, buffer gates, transmission gates 364-398, transmission gates 340-354 and a binary counter 40 which are basic logic elements used in the design of the numerous logic circuits disclosed in Borgen.

The present invention accomplishes the function of Borgen, but eliminates the need for the extremely complex hard wired logic circuitry of Borgen by replacing the logic circuitry with a microprocessor which executes a computer software program to generate all the logic signals needed to transfer, store and then load the crypto key and checkword into encryption device 24 using the computer software program illustrated in FIGS. 4-9, program

steps 40-156, and now claimed in claim 12.

The circuitry of Best is also hard wired in that the encryption function is performed by a random number generator 188, cipher key register 167, address scrambler 186 and gates 182 which perform an Exclusive-OR of a scrambled address with a program byte to produce a cipher byte.

It should be noted that the teaching of Best is directed to a hard wired logic circuit which encrypts a computer program whereas the present invention utilizes the computer program to run a microprocessor for the purpose of transferring storing and loading a crypto key into a missile's on board encryption unit.

While Maher teaches the use of a check bit to determine validity of the key, incorporating Maher into the Examiner proposed combination would likely require the design of additional complex logic circuitry. For example, if the hard wired logic circuit design taught by Borgen were implemented to perform the method steps of Applicants' invention there would be a requirement to add logic circuitry which more than likely would be as complex or more complex than logic circuitry for the sequencing control circuit 75. It needs to be understood that any change in the function of sequencing control circuit 75 requires a substantial change in the hard wired digital logic

circuitry of sequencing control circuit 75, a complex electronic design change which applicants respectfully submit is not obvious in view of the teachings of Borgen in view of Maher. In a like manner, the hard wired circuitry of Best would necessitate added logic circuitry which more than likely would be as complex or more complex than the logic circuitry of Borgen or Best.

Further, to include the duplication function taught by Le et al. would necessitate additional logic circuitry which more than likely would be as complex or more complex than the logic circuitry of Borgen or Best. Applicants' solves this problem by using computer software executable by microcontroller 32.

Claim 13, as amended, now recites a method step of loading the duplicate of the crypto key and the duplicate of the check word into the encryption device when the encryption device rejects the crypto key with the function being performed by the computer software program of FIGS. 4-9 under microprocessor control.

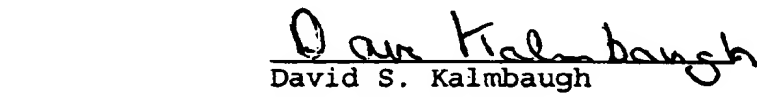
Similarly, claims 14 and 15 are being amended to recite the status of the store of the crypto key and associated check word into the memory of microcontroller 32 as being performed by the computer software within microcontroller 32 (program step 84, FIG. 6). Claims 16 and 17 are being amended to recite the status

of the erase of the crypto key and associated check word from the memory of microcontroller 32 as being performed by the computer software within microcontroller 32 (program step 124, FIG. 8).

It is respectfully submitted that claims 13-17 are in condition for allowance because they depend from claim 12 which is believed to be allowable for the reasons set forth above. In particular, it is submitted that purpose of the claims as amended, which is the use of the computer software of FIGS. 4-9 to perform each of the method steps in claim 12 and the claims dependent therefrom, is not taught or even suggested by the prior art of record.

In view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. The early allowance of claims 12, and 13-17, as amended, and the prompt issuance of this case are earnestly solicited.

Respectfully submitted,



David S. Kalmbaugh
Reg. No. 29,234
Tel.: (805) 989-8266